

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

| | | |
|--|---|---------------------|
| RITVA RAUHALA | : | CIVIL ACTION |
| | : | |
| v. | : | |
| | : | |
| GREATER NEW YORK MUTUAL INSURANCE, INC. | : | NO. 22-1788 |

MEMORANDUM OPINION

Savage, J.

October 31, 2022

Plaintiff Ritva Rauhala moves to remand this putative data breach class action removed from the state court under the Class Action Fairness Act (“CAFA”), 28 U.S.C. § 1332(d). She contends this court does not have subject-matter jurisdiction because the defendant Greater New York Mutual Insurance Company (“GNY”) has not demonstrated that she has Article III standing. She argues that GNY has not shown that she suffered an injury-in-fact, an essential requirement to establish Article III standing.

The allegations in the complaint, accepted as true, show that she has suffered an injury-in-fact, establishing Article III standing. Therefore, we shall deny the motion to remand.

Background

Rauhala settled a personal injury lawsuit against GNY’s insured.¹ As part of the payment process, Rauhala provided GNY with her Social Security number, date of birth,

¹ Compl. (Doc. No. 1, Ex. 1) ¶ 19; Pl.’s Resp. to GNY’s Mot. for Change of Venue (Doc. No. 19) at 2. On December 29, 2021, Rauhala filed a praecipe to settle, discontinue and end her personal injury lawsuit. See *Rauhala v. Penn Brooke Gardens*, Civ. A. No. 2020-19115 (C.P. Montgomery Cnty. filed Nov. 13, 2020) (Docket Entry 7).

address, medical records, billing records, and banking information.²

While Rauhala's personal injury lawsuit was pending, GNY's network and computer systems were hit by a cyberattack. From May 23 to June 1, 2021, unauthorized individuals gained access to GNY's Information Technology ("IT") system. On June 1, 2021, GNY discovered its system had been breached when employees were locked out. On October 20, 2021, GNY notified Rauhala and other claimants, customers and employees that cybercriminals had used PYSA ransomware³ to access their personally identifiable information and protected health information ("PII/PHI"). According to the notice, GNY could not rule out that data had been exfiltrated.⁴

Rauhala filed this putative class action against GNY in the Court of Common Pleas of Philadelphia County, on behalf of herself and approximately 34,000 others "impacted by the Data Breach."⁵ Asserting state law claims for negligence, unjust enrichment and invasion of privacy, she alleges that GNY failed to properly maintain and safeguard its network and computer systems to keep PII/PHI confidential and protect it from unauthorized access and disclosure. She also alleges that it failed to provide timely and adequate notice that an unauthorized third party had gained access to their confidential information.⁶

Seeking damages and injunctive relief, Rauhala alleges that as a result of the data

² Compl. ¶ 3. Before GNY could process her claim, federal law required her to provide GNY with her PII/PHI. Compl. ¶ 23; GNY's Mot. to Dismiss (Doc. No. 23) at 3 & n.3.

³ PYSA is a well-known exfiltrating ransomware utilized by cybercriminals. Compl. ¶ 29.

⁴ *Id.* ¶¶ 3, 19, 25–26, 29, 31–34.

⁵ *Id.* ¶¶ 5, 122–23, 125.

⁶ *Id.* ¶¶ 13, 51–57, 64, 71.

breach, her and class members' PII/PHI was accessed, stolen and sold on the Dark Web.⁷ She contends it is likely that the PII/PHI will be used to commit identity theft and fraud either by the cyberthieves or by those who purchase the information on the Dark Web.⁸ She claims that there is a "strong probability" that their PII/PHI has been or will be "dumped on the black market," putting them at substantial and increased risk of fraud, "actual identity theft," publication of their PII/PHI, and being targeted for future phishing, data intrusion, and other illegal schemes.⁹ She also claims damages for the loss of value of the PII/PHI¹⁰; an increase in spam calls received;¹¹ present and future out-of-pocket expenses necessary to prevent, detect and recover from attempted fraud and identity theft caused by the data breach, such as fees for credit monitoring, credit reports and credit freezes;¹² lost opportunity costs and loss of productivity associated with the time spent on these mitigation measures¹³; and anxiety, emotional distress, and loss of privacy suffered from fear of public disclosure of their PII/PHI.¹⁴ She seeks injunctive relief requiring GNY to strengthen its data security systems and monitoring procedures, submit

⁷ *Id.* ¶¶ 7–9, 77.

⁸ *Id.* ¶¶ 35–36.

⁹ *Id.* ¶¶ 78, 99–100, 101, 116, 152, 160.

¹⁰ *Id.* ¶¶ 104, 106.

¹¹ *Id.* ¶ 107.

¹² *Id.* ¶¶ 115, 152.

¹³ *Id.* ¶¶ 111–114, 152. Specifically, Rauhala alleges that they have and will have to spend time doing tasks such as closely reviewing and monitoring medical insurance accounts, bank accounts, and credit reports to identify fraudulent insurance claims, loans, and government benefits claims; placing "freezes" and "alerts" with reporting agencies; calling financial institutions, healthcare providers, government agencies and credit bureaus to dispute unauthorized and fraudulent activity in their name; and contacting financial institutions to close or modify financial accounts. *Id.* ¶ 114.

¹⁴ *Id.* ¶¶ 102–03.

to annual audits of those systems and monitoring procedures, and provide at least five years of credit monitoring.¹⁵

Analysis

The Class Action Fairness Act (“CAFA”), 28 U.S.C. § 1332(d), confers original jurisdiction over interstate¹⁶ class actions that have minimal diversity, at least 100 class members, and an amount in controversy exceeding \$5 million. 28 U.S.C. §§ 1332(d)(2), (5)(B), (6); *Dart Cherokee Basin Operating Co., LLC v. Owens*, 574 U.S. 81, 84–85 (2014) (citations omitted).

Rauhala does not argue that GNY has failed to allege facts establishing the elements of CAFA jurisdiction.¹⁷ Rather, she contends that GNY has not alleged facts showing that she suffered an injury-in-fact—a necessary element to establish Article III standing. Notably, she states that she “takes no position on whether she has Article III standing, nor does she have to, having filed in state court. It is not her burden to demonstrate standing for a forum she did not choose.”¹⁸ In response, GNY points to specific allegations in the complaint it contends constitute “concrete and particularized harm” caused by GNY’s conduct.

¹⁵ *Id.* at 39, ¶¶ 15, 120, 144.

¹⁶ See *Miss. ex rel. Hood v. AU Optronics Corp.*, 571 U.S. 161, 165 (2014) (“Congress enacted CAFA in order to ‘amend the procedures that apply to consideration of interstate class actions.’” (quoting 119 Stat. 4)).

¹⁷ Indeed, GNY has met its burden of showing that this action meets CAFA’s jurisdictional requirements. There is minimal diversity because Rauhala and GNY are citizens of different states. The case satisfies the 100-class member minimum because Rauhala alleges there are 34,000 putative class members. The aggregate amount in controversy exceeds \$5 million because her request for at least five years of credit monitoring services for the class would cost more than \$20 million.

¹⁸ Pl.’s Mot. for Remand Pursuant to 28 U.S.C. 1447(c) (Doc. No. 13) at 8 n.1; Pl.’s Reply in Supp. of Mot. for Remand (Doc. No. 24) at 2.

Standing Standard

Standing limits who can maintain a case in federal court. In the absence of standing, a plaintiff has no “case” or “controversy” empowering the federal court to exercise jurisdiction. U.S. Const. art. III, § 2. To establish Article III standing, the plaintiff must demonstrate that (1) she suffered a “concrete, particularized, and actual or imminent” injury-in-fact, (2) the injury “is fairly traceable to the challenged conduct of the defendant”; and (3) the injury would likely be redressed by a favorable judicial decision. *Spokeo, Inc. v. Robbins*, 578 U.S. 330, 338 (2016) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992)). We screen for “mere frivolity,” careful not to conflate our standing inquiry with an assessment of the merits of the plaintiff’s claim. *Adam v. Barone*, 41 F.4th 230, 233–234 (3d Cir. 2022) (quoting *Mielo v. Steak ’n Shake Ops., Inc.*, 897 F.3d 467, 478–479 (3d Cir. 2018)) (internal quotation marks and citations omitted).

To qualify as an injury-in-fact, the injury must be concrete and particularized, and actual or imminent. *Spokeo*, 578 U.S. at 339 (quoting *Lujan*, 504 U.S. at 560); *Adam*, 41 F.4th at 234 (quoting *Mielo*, 897 F.3d at 478). A concrete injury means it is real, not abstract. *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021) (quoting *Spokeo*, 578 U.S. at 340). Intangible injuries, as well as harms that are difficult to prove or measure, can be concrete. *Spokeo*, 578 U.S. at 340–341. Additionally, where the claimed injury is exposure to a substantial risk of future harm, a plaintiff can meet concreteness by alleging it caused “currently felt concrete harms.” *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 155–56 (3d Cir. 2022).

Regarding the “actual or imminent” requirement, a claim of future injury can be “imminent” if there is a “substantial risk” or “realistic danger” that the threatened harm will

occur. *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013)); *Pennell v. City of San Jose*, 485 U.S. 1, 8 (1988). Although an injury that will occur in the future is not fatal to standing, the risk of injury cannot be hypothetical or speculative. *Clemens*, 48 F.4th at 153.

“Financial harm is a ‘classic’ and ‘paradigmatic form’ of injury in fact and . . . almost always satisfies” the requirements of concrete and actual or imminent injury. *Adam*, 41 F.4th at 234 (quoting *Cottrell v. Alcon Lab’ys*, 874 F.3d 154, 163 (3d Cir. 2017)).

Recently, in *Clemens*, the Third Circuit addressed the injury-in-fact requirement in the data breach context. The court held that “where the asserted theory of injury is a substantial risk of identity theft or fraud, a plaintiff suing for damages can satisfy concreteness as long as he alleges that the exposure to that substantial risk caused additional, currently felt concrete harms.” 48 F.4th at 155–56. The court explained, “For example, if the plaintiff’s knowledge of the substantial risk of identity theft causes him to presently experience emotional distress or spend money on mitigation measures like credit monitoring services, the plaintiff has alleged a concrete injury.” *Id.* at 156. This is the injury Rauhala alleges she suffered.¹⁹

That Rauhala has not yet been victimized by theft or fraud does not preclude her having suffered an imminent injury. The *Clemens* court, noting that the “actual or imminent” requirement of the injury-in-fact prong is disjunctive, held that “a plaintiff need not wait until he or she has *actually* sustained the feared harm in order to seek judicial redress, but can file suit when the risk of harm becomes imminent.” *Clemens*, 48 F.4th at 152 (emphasis in original). The court concluded that “[t]his is especially important in

¹⁹ Compl. ¶¶ 102–03.

the data breach context, where the disclosure of the data may cause future harm as opposed to currently felt harm.” *Id.*

Rauhala has Article III standing because she has alleged harm constituting an injury-in-fact. She alleges “actual identity theft;” the “compromise, publication, and/or theft of [her] PII/PHI;” “out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of [her] PII/PHI;” “loss of value of [her] PII/PHI when it was acquired by cyber thieves in the Data Breach;” and “an increase in spam calls” as examples of “concrete and particularized harm” caused by GNY.²⁰ Her alleged damages are concrete, real and particular. They are not hypothetical or speculative. Her claimed out-of-pocket expenses alone satisfy the injury-in-fact requirement under Article III. *See Adam*, 41 F.4th at 234.

Not only does Rauhala allege actual, tangible injuries from the data breach, she claims that she is at increased risk of identity theft and fraud. She alleges that she has already suffered anxiety, emotional distress, and loss of privacy from fear of public disclosure of her PII/PHI. Thus, she has adequately plead additional concrete injuries suffered as a result of the substantial risk of identity theft in the future. *Clemens*, 48 F.4th at 155–56 (explaining that allegations that plaintiff spent time and money mitigating the fallout of a data breach constituted current concrete harms and supported that she had standing to assert a claim of exposure to future risk of identity theft).

GNY has satisfied the requirements for CAFA jurisdiction and Rauhala has Article III standing. Therefore, we shall deny Rauhala’s motion to remand.

²⁰ GNY’s Opp’n to Pl.’s Mot. for Remand (Doc. No. 21) at 2, 5.